Corporate Policy 7

Electronic and Other Business Systems

Purpose

To set forth Stryker's policy on the use of Stryker's electronic and other business systems, including, but not limited to, laptop, desktop and handheld computers; electronic mail ("e-mail"); voice mail; telephones; photographic images (digital and otherwise), personal digital assistants; video recording devices; internet access, wireless and remote system access; audio, video, and web conferencing; facsimile machines; electronic timekeeping systems and associated swipe badges; and other electronic or business equipment and services provided by Stryker to its employees (referred to in this document as "electronic and other business systems").

Scope

This Policy applies to all Stryker employees at all Stryker locations to the extent permitted by applicable law. If any provision of this Policy does not comply with local law applicable to a particular Stryker business unit, that business unit will revise this Policy to comply with applicable local law and/or implement a separate policy to comply with local law, provided that the revised policy will, to the greatest extent possible, conform with the principles contained within this Policy. All provisions of this Policy that comply with local law will remain in effect.

Basic policies

1. **Electronic and other business systems are company property:** Stryker maintains a variety of electronic and other business systems. These systems are provided to employees to assist them in the conduct of the company's business. All such systems and all documents, files, back-up copies, communications, images and recordings created on, handled by, or stored through these systems are the property of Stryker and must be properly used and protected from unintentional disclosure and unauthorized access.
2. **Access by the company:** Stryker retains the right to intercept, access, monitor, review, copy, modify, or remove from its electronic and other business systems any material generated or maintained by Stryker employees at any time and for any reason that the company deems appropriate, with or without notice to the employee. Such reasons may include, but are not limited to, conducting company business, monitoring the quality of services provided by employees, assuring compliance with company policies, ensuring security of employee personal information controls and investigating allegations of improper or illegal conduct. Material covered by this provision includes, but is not limited to, e-mail, voice mail, photographic images, telephone conversations, video recordings and computer files and documents.
3. **Access to e-mail, voice mail, and computer files by company employees:** An employee should not access or attempt to access another employee's electronic communications, voice communications or messages, or computer files without the other employee's permission or permission from the employee's supervisor. An employee should not share her/his password or logon credentials unless expressly permitted by applicable local IT department's written policies or keep it in an unprotected manner that would allow an unauthorized person access. An employee should not attempt to access, use or tamper with any confidential or personal information that is maintained upon the company's system unless they have a business authorization to do so.
4. **Disclosure of voice mail or recorded conversations:** Employees are prohibited from disclosing the contents of a recorded conversation on the company's telephone system, voice mail or other electronic and other business systems without the express consent of the company.
5. **Protection of confidential and non-public information:** Employees using electronic and other business systems will take due care to protect sensitive employee personal information and confidential and non-public information, either belonging to Stryker or in Stryker's care, from unauthorized access, disclosure, destruction, loss or alteration.

6. **Misuse of electronic and other business systems:** In addition to any requirements established by the employee's supervisor or division, employees are prohibited from using Stryker's electronic and other business systems in the following ways:
   - to make offensive, harassing, obscene, derogatory, or threatening communications
   - to download, distribute, view, publish, photograph, print or send pornographic, obscene, sexual, ethnic, religious, racial, or other form of harassing, offensive or inappropriate material
   - to install, download, distribute or send programs, files, or software of any kind, including, but not limited to chain letters, games, or computer viruses or worms, from the Internet or other outside sources without permission from the applicable IT department
   - to install, download, distribute, photograph or send materials that would violate any copyright, trademark or patent laws
   - to connect home/personal computers to the company's computer systems or conduct company business on home/personal computers or non-Stryker email without permission from the applicable IT department and the employee's supervisor
   - to make solicitations or to solicit others on behalf of any outside organizations
   - to conduct any commercial or profit-making activities that are not related to Stryker's business
   - to send any media advertisement, internet home page, electronic bulletin board posting, e-mail message, photographic image, voice mail message, or any other public representation or communication outside the company that may damage the company's reputation or the reputation of its business partners
   - for charitable endeavors unless authorized or sponsored by the company
   - to transfer any employee personal information or non-public proprietary and/or confidential information of Stryker or a company with whom Stryker does business without prior authorization of Stryker
   - to enter into any contracts or agreements on behalf of Stryker without prior authorization of the company
   - for any unreasonable personal use or any use that disrupts or interferes with the job functions of the employee or other employees
   - for any unlawful purpose or in violation of Stryker's Code of Conduct or any of the company's policies

7. **Photographic images and recordings**

   7.1. Employees are prohibited from taking photographic images, video or other recordings on company property or places in which the company does business using equipment other than electronic and other business systems maintained or owned by the company without the express consent of the company. Examples of this prohibition include the following:
      - taking photographs, digital or otherwise, using personal cameras, cell phones or other devices on company property
      - recording conversations on recording devices such as tape recorders, cell phones, or other devices
      - recording video on camcorders, cell phones or other devices

   7.2. The company reserves the right to inspect, view, listen to and obtain from employee all photographic images, videos and other recordings that an employee has taken on company property or in a place where company does business or if the company reasonably suspects that the images, videos or other recordings contain confidential or proprietary of the company or a company with whom Stryker does business.

8. **Questions concerning Stryker's Electronic and Other Business Systems Policy:** Questions concerning this Policy should be directed to the president or Human Resources director or Information Technology director of the applicable division, subsidiary, or operating unit, to Stryker's general counsel, or to Stryker's vice president of Human Resources.

9. **Violations of company policy:** Employees should notify the president or Human Resources director or Information Technology director of their division, subsidiary, or operating unit, Stryker's general counsel, or Stryker's vice president of Human Resources of any violations of this Policy. Violation of this Policy may result in disciplinary action up to and including termination.